



DEPARTMENT OF THE ARMY

U.S. Army Corps of Engineers
WASHINGTON, D.C. 20314-1000

REPLY TO
ATTENTION OF:

CEPM/CEIM-P (380-19)

27 NOV 1995

MEMORANDUM FOR ALL USACE Commands, ATTN: Directors/Chiefs of Information Management

SUBJECT: Information System Security Awareness and Interim Guidance

1. References:

a. AR 380-19, Information Systems Security, 1 August 1990.

b. MEMORANDUM, HQ USACE, CEP, 21 April 1992, Subject: Delegation of Authority for Accreditation of Automated Information Systems.

2. With the diversity of Corps' organizations and personnel involved in management, operation, and use of automated information systems (AIS), including the use of electronic transaction devices and related computer components, it is particularly important to reiterate the Corps' security policies, and to emphasize the need for instituting appropriate, common sense security practices. The Corps of Engineers Financial Management System (CEFMS), currently deploying, is, in fact, a present and very real daily challenge of effecting information security practices in what is a relative new environment of online interactive transaction based processing.

3. The Corps remains committed to implementation of AR 380-19, even while recognizing that it is currently undergoing revision at the HQDA level. The AR, in some instances, has not kept up with the pace of technology change, but its fundamental principles are sound and, therefore, briefly reiterated in this memo. Until the new AR 380-19 is published, it was also felt that Command amplification was necessary regarding areas not yet addressed by present regulation.

4. Information systems security falls into the following major areas:

a. Functional Proponent security responsibilities related to their respective automated information system(s) (AIS), which include:

(1) Risk analysis, and development of security roles and responsibilities.

(2) Development of the security plan and policies for the particular AIS.

CEPM/CEIM-P (380-19)

SUBJECT: Information Systems Security Awareness and Interim Guidance

(3) Development, testing and certification of the security capabilities native to the AIS.

b. AIS user security responsibilities related to their respective automated information system(s) (AIS), which include:

(1) Platform security awareness and practices.

(2) User ID and PASSWORD security awareness and practices.

(3) Electronic transaction device, electronic identification token, and Personal Identification Number (PIN) security awareness and practices.

5. All electronic transaction devices (including government or government issued credit cards, "electronic signature cards," certain PCMCIA cards, and electronic identification tokens) and Personal Identification Numbers (PINS) will be treated with the same degree of security consciousness required for passwords under AR 380-19 Section 2-15. These requirements are elaborated in the enclosure.

6. All AIS, regardless of mode of operation or classification of data processed, must be accredited and/or certified, as specified in AR 380-19, chapter 3. Reference b, above is still valid and delegates the accrediting authority to the lowest level possible.

7. With respect to "recycling" or "reuse" of computer components and supplies serving as non-volatile storage media, such as hard drives and floppy disks, all organizational units are reminded of the requirements of AR 380-19, Section 2-21 "Clearing, Purging, Declassifying, and Destroying Media." Adherence to this section is particularly important in light the Corps tendency to upgrade and reuse existing equipment between organizational elements. Commanders are reminded of the requirements of the Privacy Act, and of the need to safeguard proprietary or acquisition sensitive information.

8. All organizational units and AIS Functional Proponents should immediately undertake a critical security review based on this guidance, and take appropriate corrective actions, as indicated in the enclosure to restore/refresh their security consciousness.

CEPM/CEIM-P (380-19)


SUBJECT: Information Systems Security Awareness and Interim Guidance

Security practices for individual information systems will be evaluated as part of our life cycle management Milestone Decision Authority (MDA) approval process. Also, as the Headquarters undertakes its future rounds of Deputy Commanding General and Information Management Resources Oversight (IRMROP) visits, information security will be a discussion topic.

9. POC for Information Systems Security is Thomas J. Aubin, (202) 761-8723. POCs for Policy and Architectures are Larry Kennedy (202) 761-1627, or Meredith Walters (202) 761-1627.

For The Commander:

Encl


RONALD A. DABBIERI
Colonel, Corps of Engineers
Director of Information
Management


GEORGE A. FRELS
Lieutenant Colonel
Military Police
Office of Security
and Law Enforcement

ROLES/RESPONSIBILITIES

1. Electronic transaction devices are a broad category of objects allowing the individual to affect various actions under the umbrella of computer access and/or electronic commerce. Included in the category of electronic transaction devices are government credit cards such as American Express and Visa, "electronic signature" cards such as are provided for use with CEFMS, and PCMCIA cards or other electronic security tokens such as will be provided by the Defense Messaging System (DMS). Also included in this category are the Personal Identification Numbers (PINs) associated with such devices - whether government generated and assigned, or personally selected. The following guidance elaborates upon currently existing guidance in AR 380-19, Information Systems Security.

A. All electronic transaction devices and PINS will be treated with the same degree of security consciousness required for passwords under AR 380-19 Section 2-15. Issuers of passwords/electronic transaction devices/PINs will, at the time of issuance, ensure that individual recipients are briefed on:

(1) Password/Electronic Transaction Device/PIN classification and exclusiveness.

(2) Measures to safeguard passwords/electronic transaction devices/PINs.

(3) Prohibitions against disclosure/transfer of passwords/electronic transaction devices/PINs.

(4) Requirements to inform the appropriate security officer immediately of password/electronic transaction device/PINs misuse, compromise, and/or other potentially dangerous practices/occurrences.

B. Receipt of security briefings, and acknowledgement of understanding of associated responsibilities, will be acknowledged in writing with the acknowledgement retained on file by the appropriate security officer.

2. In accordance with AR 380-19 Section 2-16, all personnel who manage, design, develop, maintain, or operate AIS will undergo a training and awareness program consisting of:

ROLES/RESPONSIBILITIES

A. An initial security training and awareness briefing for AIS managers and users, including users of electronic transaction devices. This briefing can use training material governing information systems security in general, but must also be tailored to the systems the employee will be managing or using. The briefing will cover, as a minimum:

(1) Threats, vulnerabilities, and risks associated with the system. Under this portion, specific information regarding measures to reduce the threat from malicious software (virus/trojan horse/etc) will be provided, including prohibitions against loading unauthorized software, the need for frequent backup, and the requirement to report abnormal software behavior immediately.

(2) Information systems security objectives; that is, what needs to be protected, and why.

(3) Responsibilities associated with system security and/or the security of electronic transaction devices and PINs.

(4) Information accessibility, handling, and storage considerations.

(5) Physical and environmental considerations necessary to protect the system.

(6) System data and access controls.

(7) Emergency and disaster plans.

(8) Authorized system configuration and associated configuration management requirements.

B. Periodic security and awareness which may include various combinations of:

(1) Self-paced or formal instruction.

(2) Security education bulletins.

ROLES/RESPONSIBILITIES

- (3) Security posters.
- (4) Training films and tapes.
- (5) Computer-aided instruction.

3. In support of the roles and responsibilities identified in paragraphs 1-2, Functional Proponents have total security responsibility for their respective information system(s), including:

- 1.) Executing a thorough Risk Analysis, and development of security roles and responsibilities for all levels of execution - from the user, to the enabler, to the platform and communications level.
- 2.) Development of the appropriate security plan and operating policies for the particular AIS for all levels of execution - from the user, to the enabler, to the platform and communications level.
- 3.) Development and testing of the appropriate security capabilities native to the AIS, including implementation of encryption, secure transmission protocols, and message validation.

4. In support of the roles and responsibilities identified in paragraphs 1-2, AIS users have general security responsibilities for all applications which they access or interact with including:

- 1.) Platform security awareness and practice.
- 2.) User ID and PASSWORD security awareness and practices.
- 3.) Electronic transaction device, electronic identification token, and Personal Identification Number (PIN) security awareness and practices.

5. All incidents of security compromise involving passwords, electronic transaction devices and PINS will be reported in a timely fashion to the Information Systems Security Officer (ISSO) who will promptly notify the local Provost Marshall's Office

ROLES/RESPONSIBILITIES

and/or the Corps' Information Systems Security Manager (ISSM), Mr. Tom Aubin, CEPD-ZC at (202) 761-8723 as appropriate. Initial notification may be made verbally or by e-mail in the interest of expediency, but will be followed by a written notification signed by the reporting security official.